UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,783	12/10/2004	Satoshi Kitani	275870US6PCT	8620

22850 7590 08/19/2009
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SU, SARAH	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/517,783	**Applicant(s)** KITANI ET AL.	
	Examiner Sarah Su	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Amendment C, received on 26 May 2009, has been entered into record.

2. Claims 1-22 are presented for examination.

Response to Arguments

3. Applicant's arguments filed 26 May 2009 have been fully considered but they are not persuasive.

In response to applicant's argument that Asano1 and Oishi are not properly combined, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). It is further noted that Asano1 and Oishi both generate block keys for performing encryption and that even though Asano1 does not store the keys in each block, it must be stored in a memory in order for processing to be performed.

As to claim 1, it is argued by the applicant that Shindo does not disclose acquiring a second seed by decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1. The examiner respectfully disagrees. Shindo discloses that a decryption device decrypts the encryption-resultant content data into decryption-resultant content data in response to the decryption key on a block-by-block basis (0091, lines 4-7) and that the encryption-resultant signal is of a seed (0086, lines 5-6).

As to claim 9, is it argued by the applicant that Oishi does not disclose a second block key generated on the basis of the second seed. The examiner respectfully disagrees. Oishi discloses that a block seed is assigned to each sub-module and a block key is calculated on the basis of the temporary key and the block seed, where each sub-module is then encrypted using the corresponding block key (0013, lines 1-6).

4. Applicant's arguments with respect to claims 7, 8, 20, and 21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-4, 14-17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano et al. (EP 1185020 A1 and Asano1 hereinafter) in view of Oishi et al. (EP 1039462 A2 and Oishi hereinafter), and further in view of Shindo et al. (US 2003/0065925 A1 and Shindo hereinafter).

As to claims 1, 14 and 22, Asano1 discloses a system and method for information recording and reproducing, the system and method having:

first generating means for generating a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit composing the encrypted data stored on the information-recording medium (0031, lines 2-5);

decrypting means for decrypting the encrypted data read out from said information-recording medium based on the generated second block key Kb2 (0038, lines 2-4; 0052, lines 2-3, 9-10).

Asano1 fails to specifically disclose:

acquiring means for acquiring a second seed by decrypting an encrypted second seed read out from said information-recording medium on the basis of the generated first block key Kb1;

second generating means for generating a second block key Kb2 by encrypting based on the acquired second seed.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano1, as taught by Oishi.

Oishi discloses a system and method for encrypted data transfer, the system and method having:

second generating means for generating a second block key Kb2 (i.e. storage encrypted content key) **by encrypting based on the acquired second seed** (i.e. content key) (0009, lines 11-15) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 with the teachings of Oishi by using a decrypted seed to create a block key. Oishi recites motivation by disclosing that providing for a process of assigning encryption key data to already encrypted data reduces processing time when editing is performed (0007, lines 1-5; 0008, lines 1-4). It is obvious that the teachings of Oishi would have improved the teachings of Asano1 by using a seed to create a block key in order to provide for a process where the data does not need to be re-encrypted if the content key is modified in order to reduce processing time.

Asano1 in view of Oishi fails to specifically disclose:

> **acquiring means for acquiring a second seed by decrypting an encrypted second seed read out from said information-recording medium on the basis of the generated first block key Kb1**.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by Asano1 in view of Oishi, as taught by Shindo.

Shindo discloses a system and method for encrypting information, the system and method having:

> **acquiring means for acquiring a second seed by decrypting an encrypted second seed read out from said information-recording medium**

on the basis of the generated first block key Kb1 (0009, lines 1-10; 0086, lines 4-8; 0091, lines 4-7).

Given the teaching of Shindo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 in view of Oishi with the teachings of Shindo by obtaining a seed through decryption. Shindo recites motivation by disclosing that a seed is used to generate changeable key data (0074, lines 1-7) and that the seed is necessary to create a decryption key that is the same as the encryption key (0090, lines 6-9). It is obvious that the teachings of Shindo would have improved the teachings of Asano1 in view of Oishi by acquiring a seed through decryption in order to use the seed to create a decryption key that is the same as the encryption key.

As to claims 2 and 15, Asano1 discloses:

master key generating means generates a master key on the basis of the master-key generation information (0011, lines 1-5);

recording key generating means generates first recording key K1 and second recording key K2 (i.e. device unique key) **on the basis of the generated master key** (i.e. LSI key) **and information read out from the information-recording medium** (0026, lines 3-7);

said first generating means generates said first block key Kb1 (i.e. device unique key) **by encrypting based on the generated first recording key K1 and the first seed** (0026, lines 8-10);

> **decoding means decodes encrypted data stored on the information-recording medium by decrypting based on the generated second block key Kb2** (0038, lines 2-4; 0052, lines 2-3, 9-10).

Asano1 does not expressly disclose:

> **said second generating means generates a said second block key Kb2 by encrypting based on the acquired second seed and the generated second recording key K2.**

Asano1 further discloses a system that **generates a block key by encrypting based on the acquired seed and the generated recording key** (i.e. device unique key) (0026, lines 8-10), but does not expressly disclose that a second block key is generated based on a second seed and recording key.

Given the teaching of Asano1, it would have been obvious to a person having ordinary skill in the art at the time the invention was made that generating a second block key using a second set of information is a mere duplication of parts. See MPEP 2144.04.

Asano1 in view of Oishi fails to specifically disclose:

> **said acquiring means acquires a said second seed by decrypting said encrypted second seed read out from the information-recording medium on the basis of the generated first block key Kb1.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by Asano1 in view of Oishi, as taught by Shindo.

Shindo discloses:

> **said acquiring means acquires a said second seed by decrypting said encrypted second seed read out from the information-recording medium on the basis of the generated first block key Kb1** (0009, lines 1-10; 0086, lines 4-8; 0091, lines 4-7).

Given the teaching of Shindo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 in view of Oishi with the teachings of Shindo by obtaining a seed through decryption. Please refer to the motivation recited above in respect to claims 1, 14, and 22 as to why it is obvious to apply the teachings of Shindo to the teachings of Asano1.

As to claims 3-4 and 16-17, Asano1 discloses:

> **unique key generating means generates a first title unique key and a second title unique key on the basis of the master key, a disc ID, which is information read out from the information-recording medium, and two title keys recorded on the information-recording medium** (0020, lines 2-7);
>
> **said recording key generating means generates said first recording key K1** (i.e. result) **by encrypting based on the first title unique key and first information** (i.e. block seed) **read out from the information-recording medium** (0024, lines 7-10).

7. Claims 5-6 and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano1 in view of Asano et al. (US 2002/0169971 A1 and Asano2 hereinafter) and further in view of Shindo.

As to claims 5 and 18, Asano1 discloses:

> **generate a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit** (0031, lines 2-5).

Asano1 fails to specifically disclose:

> **an authentication-processing unit configured to carry out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks;**
>
> **a plurality of encryption-processing units, at least one encryption-processing unit configured;**
>
> **acquire a second seed by reading out and decrypting an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1;**
>
> **generate output-use encrypted information by encrypting data including the second seed on the basis of the session key Ks,**
>
> **where the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks is output through an interface.**

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano1, as taught by Asano2. Asano2 discloses a system and method for data authentication, the system and method having:

an authentication-processing unit configured to carry out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks (0449, lines 10-11; 0450, lines 1-3) in order to authenticate processes between two systems;

a plurality of encryption-processing units (i.e. A,B)**, at least one encryption-processing unit configured** (0449, lines 1-2; 0451, lines 1-2) in order to process data separately;

generate output-use encrypted information (i.e. secret communication) **by encrypting data including the second seed on the basis of the session key Ks** (0451, lines 7-9) in order to provide for authenticated communication between systems;

where the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks is output through an interface (i.e. between A and B) (0451, lines 7-9) in order to provide for authenticated communication between systems.

Given the teaching of Asano2, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 with the teachings of Asano2 by encrypting data with a seed using a session key. Asano2 recites motivation by disclosing that authentication can be performed using the session key by determining if inequality is found during verification of the received data (0452, lines 1-3). It is obvious that the teachings of Asano2 would have improved the teachings of Asano1 by encrypting data with a seed using a session key in order to provide for authentication of the received data between systems.

Asano1 in view of Asano2 fails to specifically disclose:

> **acquire a second seed by reading out and decrypting an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1**.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by Asano1 in view of Asano2, as taught by Shindo.

Shindo discloses:

> **acquire a second seed by reading out and decrypting an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** (0009, lines 1-10; 0086, lines 4-8).

Given the teaching of Shindo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 in view of Asano2 with the teachings of Shindo by obtaining a seed through decryption. Please refer to the motivation recited above in respect to claims 1, 14, and 22 as to why it is obvious to apply the teachings of Shindo to the teachings of Asano1 in view of Asano2.

As to claims 6 and 19, Asano1 discloses:

> **generate a master key on the basis of master-key generation information held by the information-recording medium drive** (0011, lines 1-5);
>
> **generate two recording keys K1 and K2** (i.e. device unique key) **on the basis of the master key** (i.e. LSI key) **and information read out from the information-recording medium** (0026, lines 3-7);
>
> **generate the first block key Kb1** (i.e. device unique key) **by carrying out an encryption process based on the generated first recording key K1 and the first seed** (0026, lines 8-10).

Asano1 fails to specifically disclose:

> **acquire the second seed by decrypting the encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1**;
>
> **generate the output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks**;
>
> **output the output-use encrypted information including the second seed and the second recording key K2 through an interface**.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano1, as taught by Asano2. Asano2 discloses:

> **generate the output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks** (0451, lines 7-9) in order to provide for authenticated communication between systems;
>
> **output the output-use encrypted information including the second seed and the second recording key K2 through an interface** (0451, lines 7-9) in order to provide for authenticated communication between systems.

Given the teaching of Asano2, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 with the teachings of Asano2 by encrypting data with a seed using a session key. Please refer to the motivation recited above in respect to claims 5 and 18 as to why it is obvious to apply the teachings of Asano2 to the teachings of Asano1.

Asano1 in view of Asano2 fails to specifically disclose:

> **acquire the second seed by decrypting the encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by Asano1 in view of Asano2, as taught by Shindo.

Shindo discloses:

> **acquires a second seed by decrypting the encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** (0009, lines 1-10; 0086, lines 4-8; 0091, lines 4-7).

Given the teaching of Shindo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 in view of Asano2 with the teachings of Shindo by obtaining a seed through decryption. Please refer to the motivation recited above in respect to claims 1, 14, and 22 as to why it is obvious to apply the teachings of Shindo to the teachings of Asano1 in view of Asano2.

8. Claims 7, 8, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano2 in view of Asano1.

As to claims 7 and 20, Asano2 discloses:

> **an authentication-processing unit for carrying out an authentication process with the external apparatus outputting the encrypted data in order to generate a session key Ks** (0449, lines 10-11; 0450, lines 1-3);
>
> **acquiring a seed** (i.e. content key) **used as key generation information and a recording key** (i.e. table key) **by decrypting, based on the session key,**

said encrypted information received through the data input interface (0557, lines 9-15).

Asano2 fails to specifically disclose:

generating a block key to be used as decryption key for decryption of said encrypted data by encrypting, based on the seed and the recording;

decrypting, based on the block key, said encrypted data.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano2, as taught by Asano1.

Asano1 discloses:

generating a block key to be used as decryption key for decryption of said encrypted data by encrypting, based on the seed and the recording key (i.e. device unique key) (0026, lines 8-10) in order to recreate a key with which to restore original data;

decrypting, based on the block key, said encrypted data (0052, lines 9-10) in order to restore original data.

Given the teaching of Asano1, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano2 with the teachings of Asano1 by creating a block key from supplied data. Asano1 recites motivation by disclosing that encrypting block data with different encryption keys enhances the protection against cryptanalysis of the data (0016, lines 6-8). It is obvious that the teachings of Asano1 would have improved the teachings of Asano2 by creating a block key from supplied data in order to enhance protection against cryptanalysis.

As to claims 8 and 21, Asano2 discloses:

> **an authentication-processing unit for carrying out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks** (0449, lines 10-11; 0450, lines 1-3);
>
> **a plurality of encryption-processing units, at least one encryption-processing unit** (0449, lines 1-2; 0451, lines 1-2);
>
> **means for generating output-use encrypted information encrypting the decrypted data on the basis of the generated session key Ks** (0557, lines 5-7);
>
> **where the output-use encrypted information obtained as a result of encrypting of the decrypted data on the basis of the session key Ks is output through an interface** (0557, lines 5-11).

Asano2 fails to specifically disclose:

> **means for generating a block key on the basis of a seed serving as key generation information set for the encryption-processing unit**;
>
> **means for acquiring decrypted data by decrypting the encrypted data read out from the information-recording medium on the basis of the generated block key**.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano2, as taught by Asano1. Asano1 discloses:

> **means for generating a block key on the basis of a seed serving as key generation information set for the encryption-processing unit** (0031, lines 2-5) in order to recreate a key with which to restore original data;
>
> **means for acquiring decrypted data by decrypting the encrypted data read out from the information-recording medium on the basis of the generated block key** (0038, lines 2-4; 0052, lines 2-3, 9-10).

Given the teaching of Asano1, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano2 with the teachings of Asano1 by creating a block key from supplied data. Please refer to the motivation recited above in respect to claims 7 and 20 as to why it is obvious to apply the teachings of Asano1 to the teachings of Asano2.

9. Claims 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano1 in view of Oishi, and further in view of Shindo.

As to claim 9, Asano1 discloses:

> **generating, outside the information-recording medium** (i.e. in information recorder)**, a first seed** (i.e. ATS) **serving as key generation information set for each of encryption-processing units composing said encrypted data** (0017, lines 5-9; 0018, lines 1-5);

storing said first seed in the information-recording medium (0034, lines 5-6).

Asano1 fails to specifically disclose:

generating, outside the information-recording medium, a second seed service as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed;

storing said second seed in the information-recording medium;

generating, outside the information-recording medium, an encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed;

storing said encrypted content in the information-recording medium.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by Asano1, as taught by Oishi.

Oishi discloses:

storing said second seed in the information-recording medium (i.e. storage device) (0009, lines 8-10) in order to allow the seed to be provided**;**

generating, outside the information-recording medium, an encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed (0009, lines 3-5, 8-11; 0013, lines 1-6) in order to protect the content**;**

storing said encrypted content in the information-recording medium (0014, lines 3-5) in order to allow the encrypted content to be retrieved**.**

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 with the teachings of Oishi by using a decrypted seed based on another seed. Oishi recites motivation by disclosing that providing for a process of assigning encryption key data to already encrypted data reduces processing time when editing is performed (0007, lines 1-5; 0008, lines 1-4). It is obvious that the teachings of Oishi would have improved the teachings of Asano1 by using a seed to create a block key in order to provide for a process where the data does not need to be re-encrypted if the content key is modified in order to reduce processing time.

Asano1 in view of Oishi fails to specifically disclose:

> **generating, outside the information-recording medium, a second seed serving as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by Asano1 in view of Oishi, as taught by Shindo.

Shindo discloses:

> **generating, outside the information-recording medium, a second seed service as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed** (0009, lines 1-10; 0086, lines 4-8; 0091, lines 4-7**).**

Given the teaching of Shindo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Asano1 in view of Oishi with the teachings of Shindo by obtaining a seed through decryption. Please refer to the motivation recited above with respect to claims 1, 14, and 22 as to why it is obvious to apply the teachings of Shindo to the teachings of Asano1 in view of Oishi.

As to claim 10, Asano1 discloses:

> **where the first seed is stored inside control information set for each of encryption-processing units whereas the second seed is stored as encrypted information in a user-data area outside the control information** (0022, lines 2-3; 0023, lines 3-6).

As to claim 11, Asano1 discloses:

> **where the first seed** (i.e. seed) **is stored in a user-data area as unencrypted data whereas the second seed** (i.e. data in block) **is stored in the user-data area as part of said encrypted data** (0023, lines 3-6).

As to claim 12, Asano1 discloses:

> **where the encrypted data is a transport stream packet** (0018, lines 8-9), **the first seed is stored inside control information for a plurality of transport stream packets** (0018, lines 4-7; 0022, lines 2-3), **and the second**

seed is stored as encrypted information inside one of the transport stream packets in a user-data area outside the control information (0023, lines 3-6).

As to claim 13, Asano1 discloses:

where the first seed is stored inside a transport stream packet in a user-data area as unencrypted data whereas the second seed is stored as encrypted information inside the transport stream packet in the user-data area (0018, lines 4-10; 0023, lines 3-6).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431